

Listing of the Claims:

Claims 1-10 (cancelled).

11. (Previously Presented) A method for transmitting data, comprising:

- inverting the data to be transmitted;
- forming, according to a specifiable signature formation method, a first signature as a function of both the data to be transmitted and the inverted data;
- transmitting the first signature together with the data to a receiver;
- inverting the transmitted data at the receiver;
- forming a second signature in the receiver according to the specifiable signature formation method as a function of both the transmitted data and the inverted transmitted data;
- and
- comparing the first signature with the second signature.

12. (Previously Presented) The method as recited in Claim 11, wherein:

- at least one of the first signature and the second signature is formed in a bit-parallel manner in accordance with a signature register having multiple inputs.

13. (Previously Presented) The method as recited in Claim 11, wherein:

- at least one of the first signature and the second signature is formed over several messages.

14. (Previously Presented) The method as recited in Claim 13, wherein:

- at least one of the first signature and the second signature is transmitted by being distributed over several messages.

15. (Previously Presented) The method as recited in Claim 11, wherein:

- the data to be transmitted includes one of:
 - input data of a precision of one bit and that arrives at processing units in messages via data buses, and
 - calculation results that are redundantly generated in parallel on multiple

computers,
in order to check a match of the data only the corresponding signatures are transmitted.

16. (Previously Presented) The method as recited in Claim 11, wherein:

the method is used for checking a memory content of a memory area of one of a read-only memory, flash memory, and a read-write memory.

17. (Previously Presented) The method as recited in Claim 16, wherein:

the data of the memory content to be verified are inverted,
a first signature is formed according to the specifiable signature formation method as a function of the data to be verified and of the inverted data and is stored as a setpoint signature in the memory area of the one of the read-only memory, the flash memory, and the read-write memory,

in order to verify the transmitted data located in the memory area to be verified, the transmitted data is inverted, and

as a function of the inverted transmitted data and of the transmitted data, the second signature is formed according to the specifiable signature formation method and is compared with the setpoint signature.

18. (Previously Presented) The method as recited in Claim 11, wherein:

the method is carried out via a computer program stored on a memory element executable on one of a computing unit and a control unit corresponding to a processing unit.

19. (Previously Presented) The method as recited in Claim 18, wherein:

the memory element includes one of a random access read-write memory, a read-only memory, and a flash memory.

20. (Previously Presented) A control unit for a motor vehicle, comprising:

at least one processing unit; and

a memory element in which a computer program is stored that is executable on the at

least one processing unit, wherein when the at least one processing unit executes the computer program the following are performed:

inverting the data to be transmitted;

forming, according to a specifiable signature formation method, a first signature as a function of both the data to be transmitted and the inverted data;

transmitting the first signature together with the data to a receiver;

inverting the transmitted data at the receiver;

forming a second signature in the receiver according to the specifiable signature formation method as a function of both the transmitted data and the inverted transmitted data;
and

comparing the first signature with the second signature.